期末试题

试卷共 7 页, 共 13 题, 满分 30 分.

判断/选择题: 无需写出证明.

1. (1 分) 存在一对编码 $E : \{0,1\}^7 \to \{0,1\}^{10}$ 和解码 $D : \{0,1\}^{10} \to \{0,1\}^7$, 使得对于任何消息 $x \in \{0,1\}^7$, 即使更改 $c = E(x)$ 中的任意一位, 也能被正确解码.

   解 错误

   假设存在这样的 E, D. 令消息随机, 被更改位置也随机. 那么 D 不仅可以解码出消息, 还可以指出哪一位被更改. 总共解码出至少 $7 + \log_2(10)$ 比特的信息.

2. (1 分) 可以用三种颜色给 K_4 边染色, 使得任意两个公用顶点的边都不同色.

   解 正确

3. (1 分) X, Y 是实随机变量. 如果 $\mathrm{Var}(X) = \mathrm{Var}(Y) = \mathrm{Cov}(X, Y) < \infty$, 那么 $\exists c, \Pr[X - Y = c] = 1$.

   解 正确

   $\mathrm{Var}(X - Y) = \mathrm{Var}(X) + \mathrm{Var}(Y) - 2\,\mathrm{Cov}(X, Y) = 0$.

4. (1 分) 有两沓抽奖券, 每沓 8 张. 已知其中一沓有 4 张中奖, 另一沓有 2 张中奖. 允许选择两张抽奖券刮奖. 随机选取第一张抽奖券. 如果第一张抽奖券中奖, 第二张刮奖券应该如何选择.

   解 都一样

   如果策略是不换, 那第二次也中奖的条件概率等于

   $$\frac{\Pr[\text{两次都中奖}]}{\Pr[\text{第一次中奖}]} = \frac{\frac{1}{2}\frac{1}{\binom{8}{2}} + \frac{1}{2}\frac{\binom{4}{2}}{\binom{8}{2}}}{6/16} = \frac{1}{3}.$$

   如果策略是换, 那第二次也中奖的条件概率等于

   $$\frac{\Pr[\text{两次都中奖}]}{\Pr[\text{第一次中奖}]} = \frac{\frac{2}{8} \cdot \frac{4}{8}}{6/16} = \frac{1}{3}.$$

填空题: 无需写出证明.

5. (2 分) $\sum_{i=0}^{9} i^3 =$ _____.

   解 2025

   $\sum_{i=0}^{n} i^3 = \sum_{i=0}^{n} (i^{\overline{3}} - 3i^{\overline{2}} + i) = \frac{1}{4}n^{\overline{4}} - n^{\overline{3}} + \frac{1}{2}n^{\overline{2}} = \left(\frac{n(n+1)}{2}\right)^2$.

6. (2 分) 考虑在一个三维立方体, v 是其中一个顶点. 考虑在三维立方体顶点上的随机游走. 以 v 为起点, 每次随机移动到一个相邻顶点. 那么首次返回时间的期望是 _____.

   具体来说, 不妨用 $\{0,1\}^3$ 表示状态空间, $X_0 = v = (0,0,0)$. 求 $\mathbb{E}[\min\{t : t > 0 \wedge X_t = v\}]$.

   解 8

   因为有唯一的稳态分布 μ 且 $\mu(v) = \frac{1}{8}$, 所以从 v 出发的期望返回时间是 8.

7. (2 分) 有一组事件 $E_1, \ldots, E_n$. 已知对任意 $S \subsetneq [n]$, 有 $\Pr[\bigwedge_{i\in S} E_i] = (1/2)^{|S|}$. 求 $\Pr[\bigwedge_{i\in[n]} E_i]$ 可能的取值范围.

   解 $[0, 2^{n-1}]$

   已知条件的充要条件是: E_i 发生概率为 $1/2$; $E_1, \ldots, E_n$ 中任意 $n-1$ 个相互独立.

   考虑以下两种极端概率空间:

   - $E_1, \ldots, E_{n-1}$ 相互独立, $E_n =$ "$E_1, \ldots, E_{n-1}$ 中奇数个发生".
   - $E_1, \ldots, E_{n-1}$ 相互独立, $E_n =$ "$E_1, \ldots, E_{n-1}$ 中偶数个发生".

   都符合题目要求. $\Pr[\bigwedge_{i\in[n]} E_i]$ 分别为 0 和 2^{1-n}. 通过加权平均, 之间的任何值也都可能.

   另一方面, $\Pr[\bigwedge_{i\in[n]} E_i] \le \Pr[\bigwedge_{i\in[n-1]} E_i] = 2^{1-n}$.

解答题: 请选择 4 道作答.

8. (5 分) 设 G 是点集 $V = [n]$ 上的一个简单无向图. 图中的点形成了 k 个联通子块 $S_1, \ldots, S_k \subseteq V$. 向 G 添加 $k-1$ 条边, 使得图联通. 问有多少种不同的添加边的方法.

   提示: 如果每个联通子块都是单点集, 那么题目就是在问有标号的 k 个点组成的树的个数.

   解 使用类似 Prüfer 编码 (第 7 次作业), 构造一个从所有添边方法到 $V^{k-2} \times S_1 \times S_2 \times \cdots \times S_k$ 的双射.

   考虑以下编码过程

   - 把 $S_1, \ldots, S_k$ 都视作一个节点. 已经添加边的联通图是一个 k 点树.

- for $t = 1, \ldots, k-1$:

  找到图中标号最小的叶子节点, 记叶子是 S_{L_t}, 其邻居是 S_{P_t}, 之间的边为 $(l_t, p_t) \in S_{L_t} \times S_{P_t}$.

  将 S_{L_t} 从图中删除.

- 定义 $r_1 \in S_1, \ldots, r_k \in S_k$, 其中 $r_{L_t} = l_t$, $r_k = p_{k-1}$.

  编码为 $(p_1, \ldots, p_{k-2}, r_1, \ldots, r_k)$.

解码过程为: $(p_1, \ldots, p_{k-2})$ 包含了 $(P_1, \ldots, P_{k-2})$, 利用 Prüfer 编码的解码得到所有 (L_t, P_t), 确定了 $S_1, \ldots, S_k$ 组成的树. 进而确定所有 (l_t, p_t).

9. (5 分) 用 $\mathsf{M}_n(\mathbb{F})$ 表示所有 $\mathbb{F}$ 上的 $n \times n$ 矩阵. 用 $\mathsf{GL}_n(\mathbb{F})$ 表示所有 $\mathbb{F}$ 上的 $n \times n$ 可逆矩阵. 我们称两个矩阵 $A, B \in \mathsf{M}_n(\mathbb{F})$ 相似当且仅当 $\exists G \in \mathsf{GL}_n(\mathbb{F})$, $GAG^{-1} = B$. 相似是一个等价关系. 求在相似关系下, $\mathsf{M}_2(\mathbb{F}_q)$ 有多少个等价类. 证明你的结果.

   提示: 可以使用 Burnside 引理.

   解 考虑 $\mathsf{GL}_2(\mathbb{F}_q)$ 对 $\mathsf{M}_2(\mathbb{F}_q)$ 的群作用 $G * A = GAG^{-1}$. 题目实际上在问该群作用有多少个轨道. 根据 Burnside 引理

$$\text{轨道数} = \frac{1}{|\mathsf{GL}_2(\mathbb{F})|} \# \left\{ (G, A) \in \mathsf{GL}_2(\mathbb{F}_q) \times \mathsf{M}_2(\mathbb{F}_q) \;\middle|\; G * A = A \right\}$$

   注意到 $G * A = A$ 等价于 $AG = GA$. 记

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \qquad G = \begin{bmatrix} e & f \\ g & h \end{bmatrix}.$$

   那么 $AG = GA$ 就等价于 $(a-d)f = (e-h)b \wedge (a-d)g = (e-h)c \wedge bg = cf$. 对此我们分类讨论

   - 一种情况是 $a - d = b = c = 0$(即 $A = aI$) 或 $e - h = f = g$(即 $G = eI$). 满足 $A = aI$ 的 A 共有 q 个. 满足 $G = eI$ 的 G 共有 $q-1$ 个. 根据容斥原理, 这样的 (G, A) 对共有

$$q|\mathsf{GL}_2(\mathbb{F}_q)| + (q-1)|\mathsf{M}_2(\mathbb{F}_q)| - q(q-1) \text{ 个.}$$

   - 另一种情况下, $(a-d, b, c)$ 和 $(e-h, f, g)$ 都不全为零. 这时 $AG = GA$ 等价于 $a-d : b : c = e-h : f : g$ 也就是 $\exists \alpha \in \mathbb{F}_q, (a-d, b, c) = \alpha(e-h, f, g)$. 这种情况下符合条件的 (G, A) 对共有

$$\underbrace{(|\mathsf{GL}_2(\mathbb{F}_q)| - (q-1))}_{G \text{ 的个数}} \cdot \underbrace{(q-1)}_{\alpha} \cdot \underbrace{q}_{e} \text{ 个.}$$

   代入 $|\mathsf{M}_2(\mathbb{F}_q)| = q^4$, $|\mathsf{GL}_2(\mathbb{F})| = (q^2-1)(q^2-q)$,

$$\text{轨道数} = \frac{q|\mathsf{GL}_2(\mathbb{F}_q)| + (q-1)|\mathsf{M}_2(\mathbb{F}_q)| - q(q-1) + (|\mathsf{GL}_2(\mathbb{F}_q)| - (q-1))(q-1)q}{|\mathsf{GL}_2(\mathbb{F})|} = q^2 + q.$$

注: 根据线性代数知识, 我们可以把 $\det(xI - A)$ 看作一个 $\mathbb{F}_q[x]$ 上的多项式. 也就是 A 的特征多项式. 特征多项式是相似变化下的不变量. 因此特征多项式不同的矩阵一定不相似. 特征多项式是二次首 1 多项式, 这样的多项式有 q^2 个. 因此至少有 q^2 个等价类. 但有重根时, 特征多项式相等的两个矩阵不一定相似. 实际情况见下表. 表中已经找到了 $q^2 + q$ 个等价类, 因此我们知道没有遗漏.

特征根	重根	重根	两个不等根	无根 (在 $\mathbb{F}_{q^2}$ 中有两个不等根)
特征多项式	$(x-\lambda)^2$	$(x-\lambda)^2$	$(x-\lambda_1)(x-\lambda_2)$	x^2+ax+b
代表元	$\begin{bmatrix}\lambda & \\ & \lambda\end{bmatrix}$	$\begin{bmatrix}\lambda & 1 \\ & \lambda\end{bmatrix}$	$\begin{bmatrix}\lambda_1 & \\ & \lambda_2\end{bmatrix}$	$\begin{bmatrix}a & 1 \\ -b & \end{bmatrix}$
等价类个数	q	q	$\binom{q}{2}$	$(q^2-q)/2$

另一种解法 形如 aI 的矩阵与任何矩阵交换, 单独构成一个等价类. 这样的等价类有 q 个. 对于其它等价类, 我们证明它们都包含恰好一个形如 $\begin{bmatrix}a & 1 \\ b & 0\end{bmatrix}$ 的矩阵. 所以另有 q^2 个等价类.

令 $\mathcal{C}$ 表示一个等价类, 且 $\forall a, \mathcal{C} \neq \{aI\}$. 从其中选取一个矩阵 $\begin{bmatrix}a & c \\ b & d\end{bmatrix}$.

- 可以要求 b, c 不都为 0.

  如果 b, c 都为零, 那么 $a \neq d$. 改为选取 $\begin{bmatrix}1 & 1 \\ 0 & 1\end{bmatrix}\begin{bmatrix}a & 0 \\ 0 & d\end{bmatrix}\begin{bmatrix}1 & -1 \\ 0 & 1\end{bmatrix} = \begin{bmatrix}a & d-a \\ 0 & d\end{bmatrix} \in \mathcal{C}$.

- 可以要求 $b \neq 0$.

  如果 $b = 0$, 那么 $c \neq 0$. 改为选取 $\begin{bmatrix}0 & 1 \\ 1 & 0\end{bmatrix}\begin{bmatrix}a & 0 \\ c & d\end{bmatrix}\begin{bmatrix}0 & 1 \\ 1 & 0\end{bmatrix} = \begin{bmatrix}d & c \\ 0 & a\end{bmatrix} \in \mathcal{C}$.

- 可以要求 $b \neq 1$.

  如果 $b \neq 1$, 改为选取 $\begin{bmatrix}1 & 0 \\ 0 & b\end{bmatrix}\begin{bmatrix}a & b \\ c & d\end{bmatrix}\begin{bmatrix}1 & 0 \\ 0 & b^{-1}\end{bmatrix} = \begin{bmatrix}a & 1 \\ bc & d\end{bmatrix} \in \mathcal{C}$.

- 可以要求 $d = 0$.

  如果 $d \neq 0$, 改为选取 $\begin{bmatrix}1 & 0 \\ -d & 1\end{bmatrix}\begin{bmatrix}a & 1 \\ c & d\end{bmatrix}\begin{bmatrix}1 & 0 \\ d & 1\end{bmatrix} = \begin{bmatrix}a+d & 1 \\ c-da & 0\end{bmatrix} \in \mathcal{C}$.

以上说明 $\mathcal{C}$ 中含有一个形如 $\begin{bmatrix}a & 1 \\ b & 0\end{bmatrix}$ 的矩阵.

另一方面, 这个矩阵的特征多项式是 $x^2 + ax - b$. 这个形状的的矩阵的特征多项式两两不同. 而特征多项式又是相似变换下的不变量. 因此 $\mathcal{C}$ 包含恰好一个这个形状的矩阵.

10. (5 分) 设 $X_1, \ldots, X_n, Y_1, \ldots, Y_n$ 是 $2n$ 个独立的随机变量. $X_i \sim \mathrm{Bern}(4/5)$, $Y_i \sim \mathrm{Bern}(1/2)$. 求最小的不依赖于 n 的常数 c 使得 $\Pr[\sum_{i=1}^n X_i \leq \sum_{i=1}^n Y_i] \leq O(c^n)$.

解 定义 $Z_i = X_i - Y_i$, 显然 $Z_1, \ldots, Z_n$ 独立同分布. 题目所求即 $\Pr[\sum_i Z_i \le 0]$ 的概率. 令 P 表示 Z_i 的分布. 那么 $P(1) = 4/10, P(0) = 1/2, P(-1) = 1/10$. 定义分布 P_t 为 $P_t(x) \propto P(x)e^{xt}$.

根据 Sanov 或者 Cramér's theorem (第 8 次作业), $\Pr[\sum_i Z_i \le 0] \le \exp(-nD(P_{t^*} \| P))$, 其中 P_{t^*} 的期望是 0, 且这个界在指数上的常数是紧的.

不难解得 $P_{t^*}(1) = 2/9, P_{t^*}(0) = 5/9, P_{t^*}(-1) = 2/9$. 于是 $D(P_{t^*} \| P) = \log \frac{10}{9}$, 对应常数 $c = \frac{9}{10}$.

11. (5 分) 对于函数 $f : \{0,1\}^n \to \mathbb{R}$, 它的傅里叶系数 $\hat{f} : \{0,1\}^n \to \mathbb{R}$ 满足

$$\hat{f}(y) = \frac{1}{2^n} \sum_x f(x)\chi_y(x), \qquad f(x) = \sum_y \hat{f}(y)\chi_y(x).$$

考虑一个 "噪音算子" $T_\rho : (\{0,1\}^n \to \mathbb{R}) \to (\{0,1\}^n \to \mathbb{R})$, 其中 $\rho \in [0,1]$.

$$T_\rho(f)(x) = \mathop{\mathbb{E}}_{y \sim (\mathrm{Bern}(\rho))^n} \Big[f(x \oplus y) \Big].$$

求 $\widehat{T_\rho(f)}(y)$. 化简后的表达式不应该出现 $\sum$ 或 $\mathbb{E}$.

解

$$\begin{aligned}
\widehat{T_\rho(f)}(y) &= \mathop{\mathbb{E}}_x \Big[T_\rho(f)(x)\chi_y(x) \Big] \\
&= \mathop{\mathbb{E}}_x \mathop{\mathbb{E}}_{z \sim (\mathrm{Bern}(\rho))^n} \Big[f(x+z)\chi_y(x) \Big] \\
&= \mathop{\mathbb{E}}_x \mathop{\mathbb{E}}_{z \sim (\mathrm{Bern}(\rho))^n} \Big[f(x)\chi_y(x+z) \Big] \\
&= \mathop{\mathbb{E}}_x \mathop{\mathbb{E}}_{z \sim (\mathrm{Bern}(\rho))^n} \Big[f(x)\chi_y(x)\chi_y(z) \Big] \\
&= \mathop{\mathbb{E}}_x \Big[f(x)\chi_y(x) \Big] \mathop{\mathbb{E}}_{z \sim (\mathrm{Bern}(\rho))^n} \Big[\chi_y(z) \Big] \\
&= \hat{f}(y) \prod_i \mathop{\mathbb{E}}_{z_i \sim \mathrm{Bern}(\rho)} [(-1)^{y_i z_i}] \\
&= \hat{f}(y)(1-2\rho)^{\|y\|_1}
\end{aligned}$$

12. (5 分) 对一个马尔可夫链 P, 用 π 表示它的一个稳态分布, 用 $\tau(\varepsilon)$ 表示它的混合时间.

$$\tau(\varepsilon) = \text{smallest } t \text{ s.t. } d(t) \le \varepsilon$$
$$d(t) = \max_x \Delta_{\mathrm{TV}}(P^t(x,\cdot), \pi)$$

证明, 对任意 $\varepsilon > 0$, $\tau(2\varepsilon^2) \le 2\tau(\varepsilon)$.

解 固定 ε, 记 $\tau = \tau(\varepsilon)$.

用 coupling 方法证明题目. 对任意 x_0, 构造 $X_0, X_\tau, X_{2\tau}, Y_0, Y_\tau, Y_{2\tau}$, 使得 $X_0 = x_0$, $Y_0 \sim \pi$, 两边的边缘分布都是马尔可夫链 (即 $\Pr[Y_\tau = y_\tau, Y_{2\tau} = y_{2\tau} | Y_0 = y_0] = P^\tau(y_0, y_\tau)P^\tau(y_\tau, y_{2\tau})$, 对 X_t 类似), 并且 $\Pr[X_{2\tau} \ne Y_{2\tau}] \le 2\varepsilon^2$.

因为 $\Delta_{\mathrm{TV}}(X_\tau, Y_\tau) = \Delta_{\mathrm{TV}}(P^t(x_0,\cdot),\pi) \le \varepsilon$, 所以通过 coupling 可以令 $\Pr[X_\tau = Y_\tau] \ge 1-\varepsilon$.

如果 $X_\tau = Y_\tau$, 可以让两个马尔可夫链保持相同, $\Pr[X_{2\tau} = Y_{2\tau} \mid X_\tau = Y_\tau] = 1$.

如果 $X_\tau = x \ne y = Y_\tau$, 这时 $X_{2\tau}, Y_{2\tau}$ 的条件分布分别是 $P^t(x,\cdot), P^t(x,\cdot)$. 因为

$$\Delta_{\mathrm{TV}}(P^t(x,\cdot), P^t(y,\cdot)) \le \Delta_{\mathrm{TV}}(P^t(x,\cdot),\pi) + \Delta_{\mathrm{TV}}(P^t(y,\cdot),\pi) \le 2\varepsilon,$$

可以通过 coupling 令 $\Pr[X_{2\tau} = Y_{2\tau} \mid X_\tau = x, Y_\tau = y] \ge 1-2\varepsilon$.

于是

$$\Pr[X_{2\tau} \ne Y_{2\tau}] = \Pr[X_{2\tau} \ne Y_{2\tau} \mid X_\tau \ne Y_\tau] \Pr[X_\tau \ne Y_\tau] \le 2\varepsilon^2.$$

13. (5 分) 假设 n 足够大. 证明存在不依赖 n 的常数 $\alpha > 0$, 使得

采样有 αn 条边的随机图 $G \sim G(n, \alpha n)$, 并采样两个不同的随机点 u, v. 那么 u, v 在 G 上联通的概率不超过 $1/n$.

解 不妨先采样 (u, v). 考虑 G 中, 从 u 到 v 的简单 (无重复点) 的路径个数的期望.

$$\begin{aligned}
\mathbb{E}[\#\text{paths from } u \text{ to } v] &= \sum_{\ell=1}^{n} \mathbb{E}[\#\text{length-}\ell \text{ paths from } u \text{ to } v] \\
&= \sum_{\ell=1}^{n} \sum_{w_1,\ldots,w_{\ell-1}} \Pr[uw_1w_2\ldots w_{\ell-1}v \text{ is a path}] \\
&\le \sum_{\ell=1}^{n} (n-2)^{\ell-1} \Big(\frac{\alpha n}{\binom{n}{2}}\Big)^{\ell} \\
&\le \frac{1}{n} \sum_{\ell=1}^{n} (2\alpha)^{\ell} \\
&= \frac{1}{n} \frac{1}{(2\alpha)^{-1} - 1}.
\end{aligned}$$

根据 Markov bound,

$$\Pr[u, v \text{ 联通}] = \Pr[\#\text{paths from } u \text{ to } v \ge 1] \le \frac{1}{n} \frac{1}{(2\alpha)^{-1} - 1}.$$

选取 $\alpha = 1/4$ 便可以满足题目要求.

另一种解法 无放回采样 K_n 中的边 $e_1, e_2, e_3, \ldots$. 记 $G_{a:b} = (V, \{e_a, \ldots, e_b\})$, 那么 $G_{a:b} \sim G(n, b-a+1)$.

用 p_m 表示 e_{m+1} 的两个端点在 $G_{1:m}$ 中联通的概率. 这个概率随着 m 的增加单调递增, 因为它也可以看作 e_1 的两个端点在 $G_{2:m+1}$ 中联通的概率.

用 c_m 表示 $G_{1:m}$ 中环的数目的期望.

$$\begin{aligned}
c_m &= \sum_{k=3}^{n} \frac{n^{\underline{k}}}{2k} \Pr[v_1, \ldots, v_k \text{ 按此顺序构成一个环}] \\
&\le \sum_{k=3}^{n} \frac{n^{\underline{k}}}{2k} \Big(\frac{m}{\binom{n}{2}}\Big)^{k} \\
&\le \sum_{k=3}^{n} \frac{1}{6} \Big(\frac{2m}{n}\Big)^{k}.
\end{aligned}$$

注意到, 如果 e_{m+1} 的两个端点在 $G_{1:m}$ 中联通, 那么 $G_{1:m+1}$ 至少比 $G_{1:m}$ 多含有一个环. 因此

$$c_{m+1} \geq c_m + p_m, \qquad c_{2m} \geq c_m + \sum_{i=m}^{2m-1} p_i \geq m p_m, \qquad p_m \leq \frac{c_{2m}}{m}.$$

可以选择 $\alpha = 1/4$

$$p_{\alpha n} \leq \frac{c_{2\alpha n}}{\alpha n} \leq \frac{\frac{1}{6}(2\alpha)^3}{\alpha n(1-2\alpha)} = \frac{1}{6n}.$$

所求概率为,

$$\begin{aligned} \Pr[u, v \text{ 在 } G_{\alpha n} \text{ 中联通}] &\leq \Pr\Big[(u,v) \in G_{\alpha n}\Big] + \Pr\Big[u, v \text{ 在 } G_{\alpha n} \text{ 中联通} \;\Big|\; (u,v) \notin G_{\alpha n}\Big] \\ &= \frac{\alpha n}{\binom{n}{2}} + p_{\alpha n} \leq \frac{1}{n}. \end{aligned}$$